Changes to Cybersecurity Across the Navy

AFCEA Monthly Luncheon

18 August 2015

Presented by:

Mr. Brian Marsh
Assistant Chief Engineer
(Certification & Mission Assurance)
SPAWAR 5.0

Statement A: Approved for public release, distribution is unlimited (14 Aug 2015)

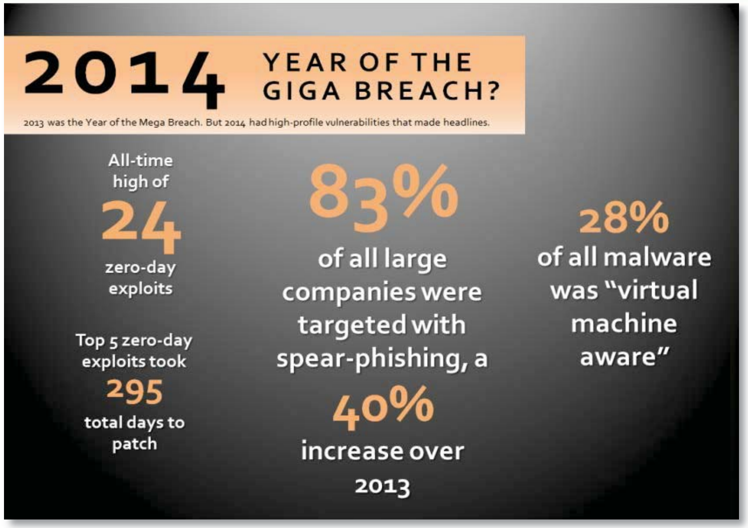
The Navy's Information Dominance Systems Command

SPAWAR

Current Cyber Environment

(Updated since my Apr 2015 AFCEA C4ISR Symposium presentation)

IAVMs and CTOs on pace to at least meet 2013 and 2014 numbers



2014 YEAR OF THE GIGA BREACH?

2013 was the Year of the Mega Breach. But 2014 had high-profile vulnerabilities that made headlines.

All-time high of **24** zero-day exploits

Top 5 zero-day exploits took **295** total days to patch

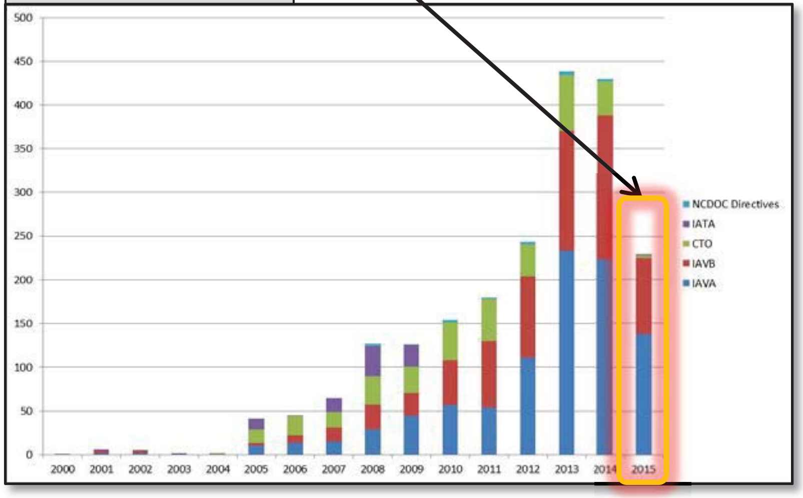
83% of all large companies were targeted with spear-phishing, a **40%** increase over 2013

28% of all malware was "virtual machine aware"

Source: Symantec 2015 Internet Security Threat Report

Major Cyber Attacks Since AFCEA C4ISR Symposium (Apr 15)

Last Update: 6 Jul 15



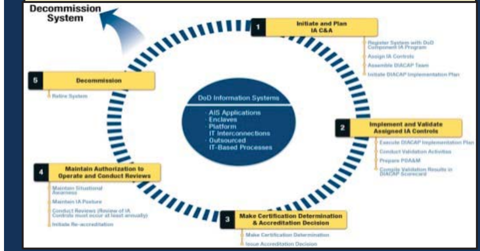
Major Cyber Attacks:
Anthem.
TARGET.
SONY PICTURES
THE HOME DEPOT
JOINT CHIEFS OF STAFF
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Extreme challenge to keep pace with the exponential increase in cyber security requirements

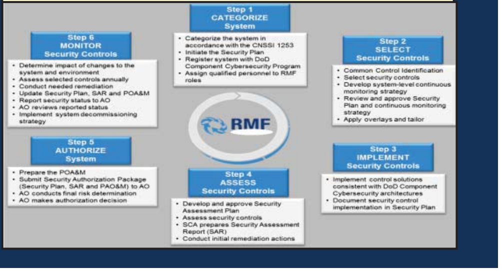
Major Changes to Navy Cybersecurity

System Certification

DIACAP


Decommission System
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Prepare POA&M
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness
Maintain IA Posture
Conduct Reviews (Review of IA Controls must occur at least annually)
Initiate Re-accreditation
5 Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform
IT Interconnections
Outsourced
IT-Based Processes

RMF



Step 1 CATEGORIZE System
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls
- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

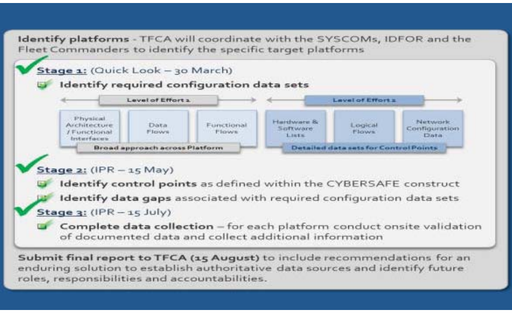
Step 3 IMPLEMENT Security Controls
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System
- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and PAO&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Cyber Baseline Configuration


Level of Effort 1
Physical Architecture / Functional Interfaces
Data Flows
Functional Flows
Broad approach across Platform
Level of Effort 2
Hardware & Software Lists
Logical Flows
Network Configuration Data
Detailed data sets for Control Points

Identify platforms - TFCA will coordinate with the SYSCOMs, IDFOR and the Fleet Commanders to identify the specific target platforms

✓ Stage 1: (Quick Look – 30 March)
- ☑ **Identify required configuration data sets**

✓ Stage 2: (IPR – 15 May)
- ☑ **Identify control points** as defined within the CYBERSAFE construct
- ☑ **Identify data gaps** associated with required configuration data sets

✓ Stage 3: (IPR – 15 July)
- ☑ **Complete data collection** – for each platform conduct onsite validation of documented data and collect additional information

Submit final report to TFCA (15 August) to include recommendations for an enduring solution to establish authoritative data sources and identify future roles, responsibilities and accountabilities.

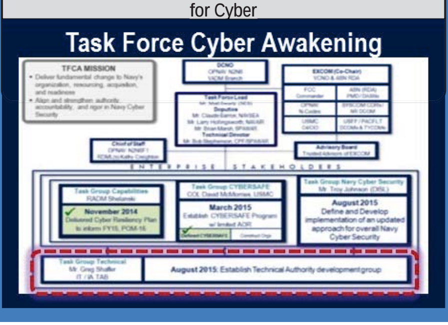
Build and implement a lasting, feasible, and repeatable CM solution

CYBERSAFE

SYSCOM-/Program-unique security controls
Systems segregated by enclave

The Navy's Information Dominance Systems Command
SPAWAR
NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL AIR SYSTEMS COMMAND
NAVAIR
MARINE CORPS SYSTEMS COMMAND
NAVFAC
Naval Facilities Engineering Command
NAVSUP
NAVAL SUPPLY SYSTEMS COMMAND

Recognition of the Need for a Centralized Navy Plan for Cyber



Task Force Cyber Awakening

TFCA MISSION
- Deliver fundamental change to Navy's organization, resourcing, acquisition, and readiness
- Align and strengthen authority, accountability, and rigor in Navy Cyber Security

DCNO
OPNAV N2N6
VADM Branch

EXCOM (Co-Chair)
VCNO & ASN RDA

FCC Commander	ASN (RDA) PMD / DASNs
OPNAV N-Codes	SYSCOM CDRs / NR DCOM
USMC DirC4/CIO	USFF / PACFLT ECOMs & TYCOMs

Task Force Lead
Mr. Matt Swartz (SES)
Deputies
Mr. Claude Barron, NAVSEA
Mr. Larry Hollingsworth, NAVAIR
Mr. Brian Marsh, SPAWAR
Technical Director
Mr. Bob Stephenson, CPF/SPAWAR

Chief of Staff
OPNAV N2N6F1
RDML(s) Kathy Creighton

Advisory Board
Trusted Advisors of EXCOM

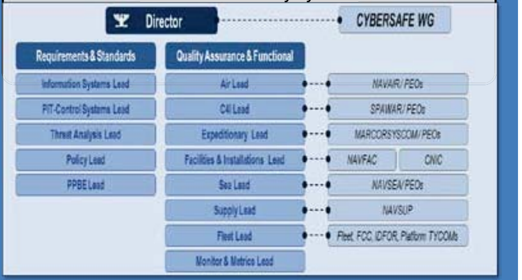
Task Group Capabilities
RADM Shelanski
✓ November 2014
Delivered Cyber Resiliency Plan to inform FY15, POM-16

Task Group CYBERSAFE
COL David McMorries, USMC
March 2015
Establish CYBERSAFE Program w/ limited AOR
✓ Defined CYBERSAFE | Construct Orgs

Task Group Navy Cyber Security
Mr. Troy Johnson (DISL)
August 2015
Define and Develop implementation of an updated approach for overall Navy Cyber Security

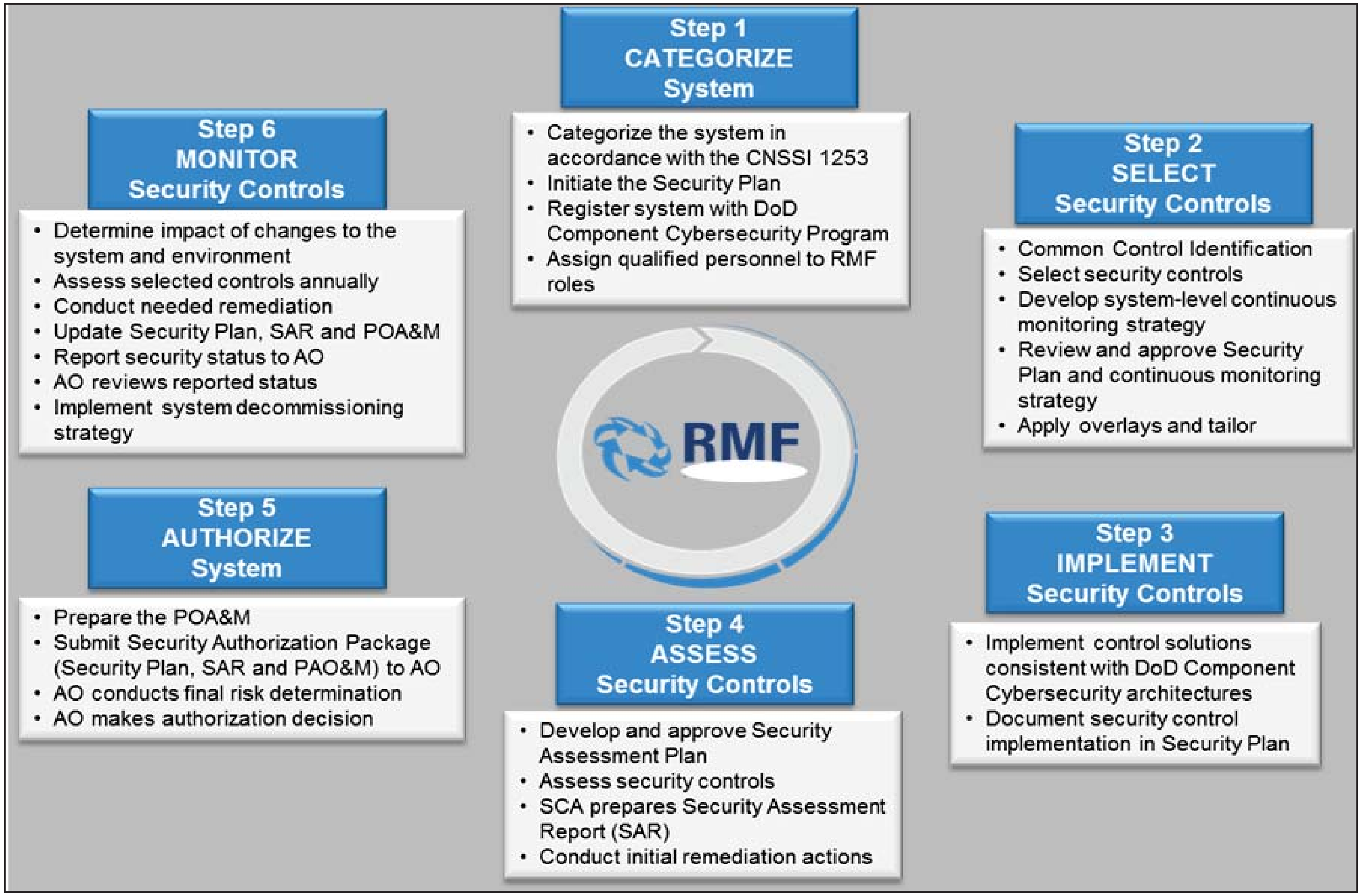
Task Group Technical
Mr. Greg Shaffer
IT / IA TAB
August 2015: Establish Technical Authority development group

CYBERSAFE addresses security controls for a subset of mission critical Navy systems



SPAWAR-led IT/IA Technical Authority Board (TAB) Plays a Key Role in Each

Risk Management Framework (RMF)



Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and PAO&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Cannot Mitigate Every Vulnerability—RMF Provides a Means to Understanding Risk and Enables a Full DOTMLPF Approach to Cybersecurity (Protect, Detect, Respond)

Baseline Configuration

Critical to Understanding Cyber Risk

Standards

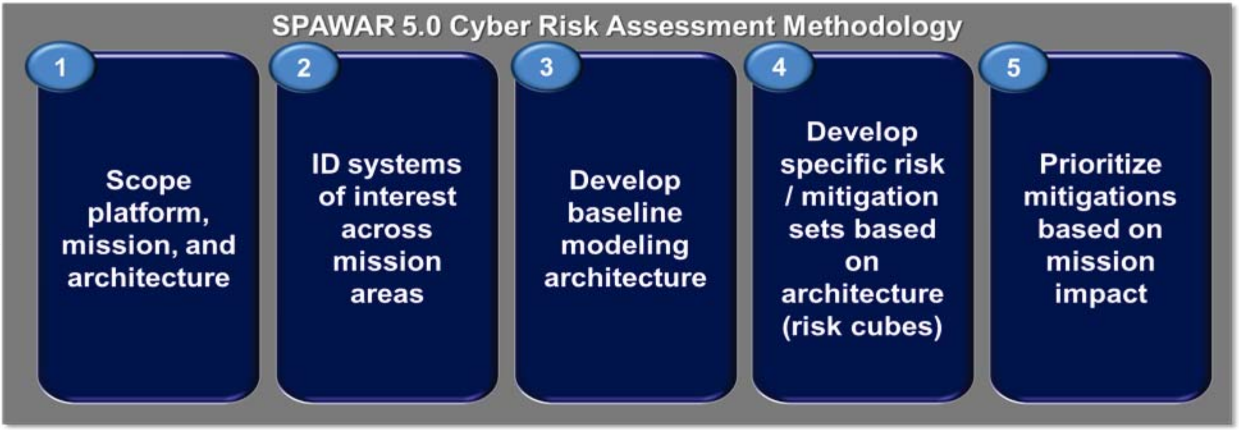
- IT/IA TAB endorse data standard, invoke to support CM
- Institute policies to ensure SYSCOM, POR compliance w/ standard

Material Controls

- Establish strict material, configuration controls of selected cyber configuration items
- Implement processes to assist Fleet w/ Cyber CM
- Leverage FCC pilot tools to audit/validate operational use of certified baselines

Certification

- Integrate pilot events into cyber security inspections and CYBERSAFE certifications

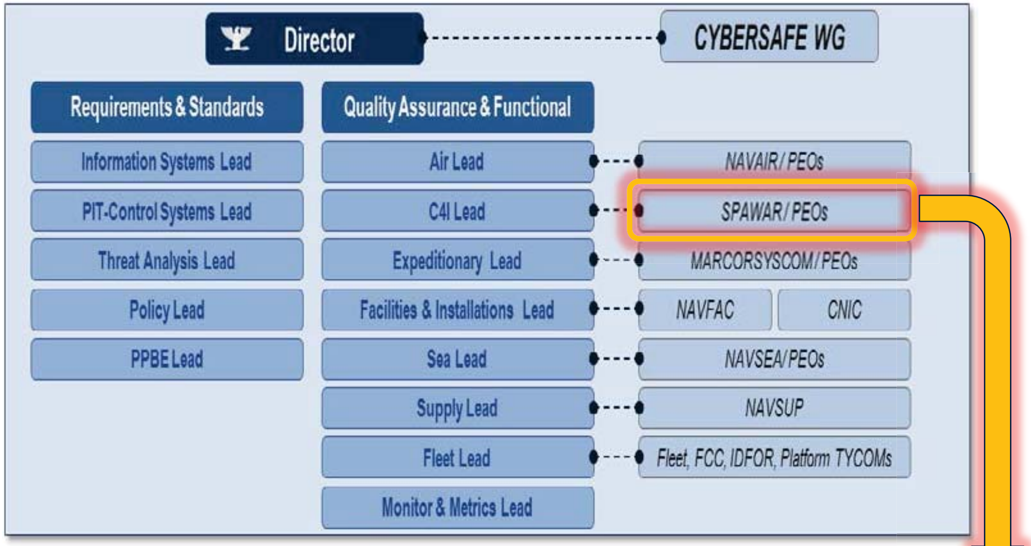


SPAWAR 5.0 Cyber Risk Assessment Methodology

1. Scope platform, mission, and architecture
2. ID systems of interest across mission areas
3. Develop baseline modeling architecture
4. Develop specific risk / mitigation sets based on architecture (risk cubes)
5. Prioritize mitigations based on mission impact

Cyber Risk = *ƒ*(Threat, Vulnerability, Consequence)

CYBERSAFE



Director

CYBERSAFE WG

Requirements & Standards

Information Systems Lead

PIT-Control Systems Lead

Threat Analysis Lead

Policy Lead

PPBE Lead

Quality Assurance & Functional

Air Lead

C4I Lead

Expeditionary Lead

Facilities & Installations Lead

Sea Lead

Supply Lead

Fleet Lead

Monitor & Metrics Lead

NAVAIR/PEOs

SPAWAR/PEOs

MARCORSYSCOM/PEOs

NAVFAC

CNIC

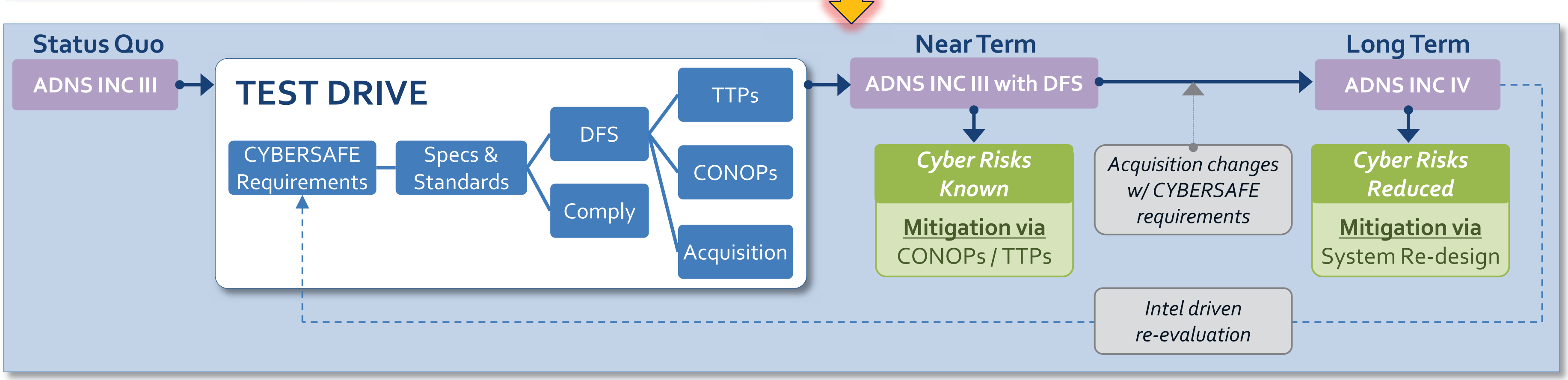
NAVSEA/PEOs

NAVSUP

Fleet, FCC, IDFOR, Platform TYCOMs

ADNS "Test Drive" of CYBERSAFE Processes

- Ensure we have the right management construct, processes and policies to execute CYBERSAFE



Status Quo

ADNS INC III

TEST DRIVE

CYBERSAFE Requirements

Specs & Standards

DFS

Comply

TTPs

CONOPs

Acquisition

Near Term

ADNS INC III with DFS

Cyber Risks Known

Mitigation via

CONOPs / TTPs

Acquisition changes w/ CYBERSAFE requirements

Long Term

ADNS INC IV

Cyber Risks Reduced

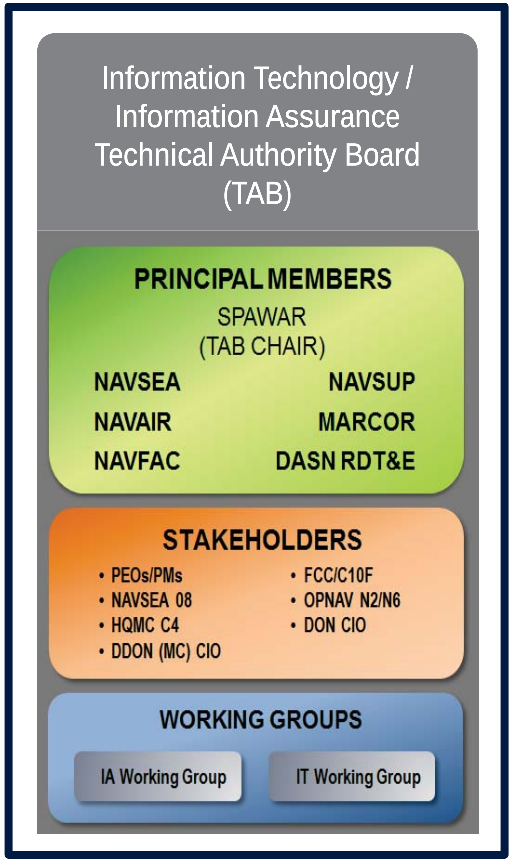
Mitigation via

System Re-design

Intel driven re-evaluation

CYBERSAFE Program will focus on *Mission Assurance* of critical warfighting capabilities

Information Technology (IT) / Information Assurance (IA) Technical Authority Board (TAB)



Information Technology / Information Assurance Technical Authority Board (TAB)

PRINCIPAL MEMBERS

SPAWAR
(TAB CHAIR)

NAVSEA	NAVSUP
NAVAIR	MARCOR
NAVFAC	DASN RDT&E

STAKEHOLDERS

- PEOs/PMs
- NAVSEA 08
- HQMC C4
- DDON (MC) CIO
- FCC/C10F
- OPNAV N2/N6
- DON CIO

WORKING GROUPS

IA Working Group

IT Working Group

With SPAWAR assigned as the Navy’s IT and IA Technical Authority, the TAB plays a critical role in:

▼ RMF

- Security Controls Assessor role and criteria/processes
- Cybersecurity technical warrants issued to other SYSCOM SCAs

▼ Cyber Baseline Configuration

- Use baseline configuration data to perform end-to-end cyber risk assessments of whole platforms and potential impact to operational missions
- Hold Ship Commanding Officers accountable to maintain CM

▼ CYBERSAFE

- Provide the criteria, specifications and standards to support CYBERSAFE

The TAB’s Cybersecurity Imperative:
View Our Systems and Networks the Same Way Our Adversaries Do!